Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

# VPN BROADBAND LAN SHARING WITH WI-FI NANO BASED USB ADAPTER

Atvar Singh [1] | C.Er. Harisharan Aggarwal [2]

[1] Department of Electronics and Communication Engg., Guru Gobind Singh College Of Engg. & Technology, Guru kashi University, Talwandi sabo, Bathinda, Punjab, India.

[2] HOD, Department of Electronics and Communication Engg., Guru Gobind Singh College Of Engg. & Technology, Guru kashi University, Talwandi sabo, Bathinda, Punjab, India

## ABSTRACT

Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN (wimax) technology to enable remote users to securely connect to a private network. Many corporations are very seriously concerned about VPN security of networks. In this regards, the VPN (wimax) modem and antenna standard was developed to the standard address the security problems, no doubts virtual private networking is famous for good security for the clients past few years. But VPN Broadband connection is a major problem not make a multiuser clients, because it is a single user. In the thesis work ,VPN (wimax) broadband internet connect through Wi-Fi on android mobile with the help of nano technology based mini adapter clients sharing a broadband LAN also we make with the help of nano adapter make a multiuser

**KEYWORDS:** Wimax antenna, Broadband VPN, Nano mini adapter(IEEE 802.11)

## I. INTRODUCTION

A Virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

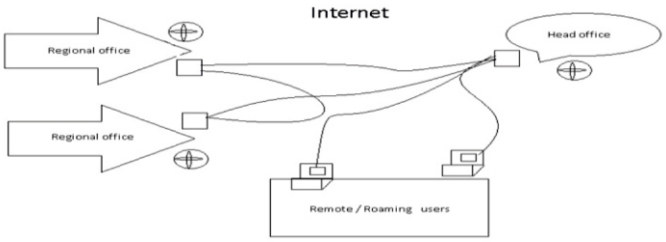


**Fig 1 Internet VPN**

Virtual Private Networks may allow employees to securely access a Corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support connect broadcast domains, services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN).

## II. ADVANTAGES & DISADVANTAGES

A VPN is a inexpensive effective way of building a private network. The use of the Internet as the main communications channel between sites is a cost effective alternative to expensive leased private lines. The costs to a corporation include the network authentication hardware and software used to authenticate users and any additional mechanisms such as authentication tokens or other secure devices. The relative ease, speed, and flexibility of VPN provisioning in comparison to leased lines makes VPNs an ideal choice for corporations who require flexibility. For example, a company can adjust the number of sites in the VPN according to changing requirements.

There are several potential disadvantages with VPN use. The lack of Quality of Service (QOS) management over the Internet can cause packet loss and other performance issues. Adverse network conditions that occur outside of the private network is beyond the control of the VPN administrator. For this reason, many large corporations pay for the use of trusted VPNs that use a private network to guarantee QOS. Vendor interoperability is another potential disadvantage as VPN technologies from one vendor may not be compatible with VPN technologies from another vendor. Neither of these disadvantages has prevented the widespread acceptance and deployment of VPN technology.

## III. RESEARCH METHODLOGY

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys.

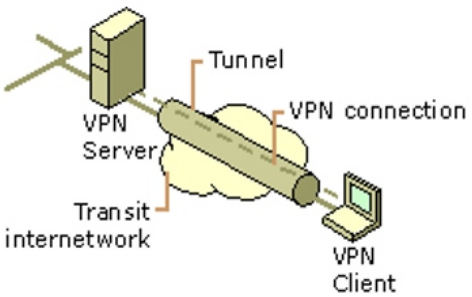


**Fig 2 Virtual private network connections**

VPN connections allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN connection is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network link between the sites.

In both of these cases, the secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network.

VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and must be able to communicate with each other.

To provide employees with the ability to connect to corporate computing resources, regardless of their location, a corporation must deploy a scalable remote access solution. Typically, corporations choose either an MIS department solution, where an internal information systems department is charged with buying, installing, and maintaining corporate modem pools and a private network infrastructure; or they choose a value-added network solution, where they pay an outsourced company to buy, install, and maintain mod modem pools.

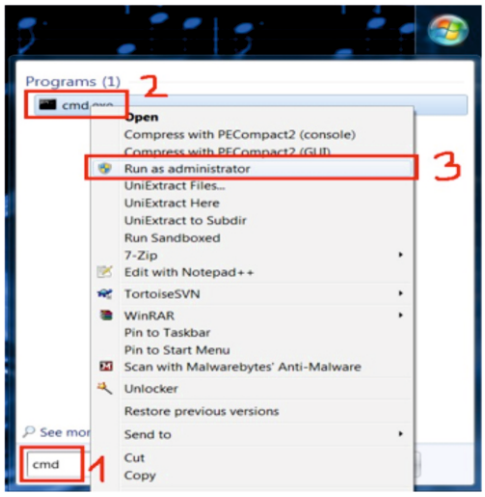


**Fig 3 Cmd command run as administrator**

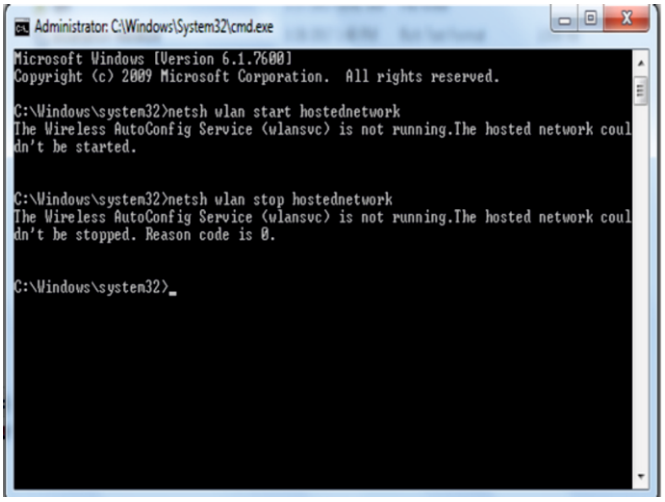


**Fig 4 Hostednetwork Couldn,t Start/Stop Network**

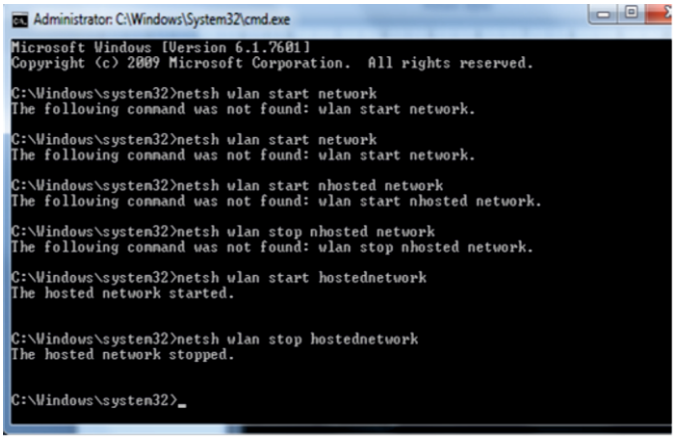


**Fig 5 netsh wlan start/stop hostednetwork**

Type the following commands into Windows console: netsh wlan set hostednetwork mode=allow ssid=atvar=12345678 netsh wlan start hostednetwork

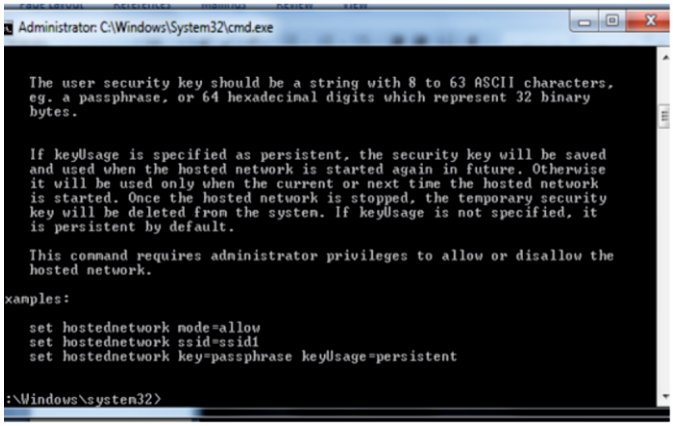


**Fig 6 Administrator privileges to allow or disallow**

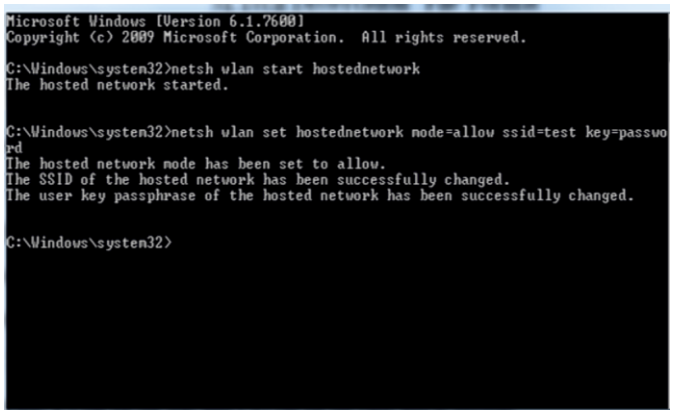


**Fig 7 Hosted network successfully configured**

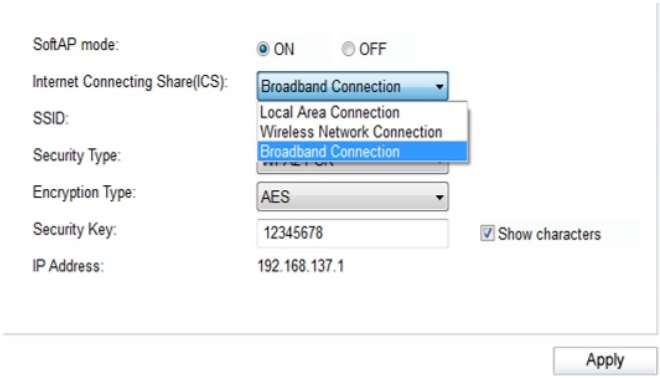


**Fig 8 Sharing command shows broad band, LAN and wireless network connection**

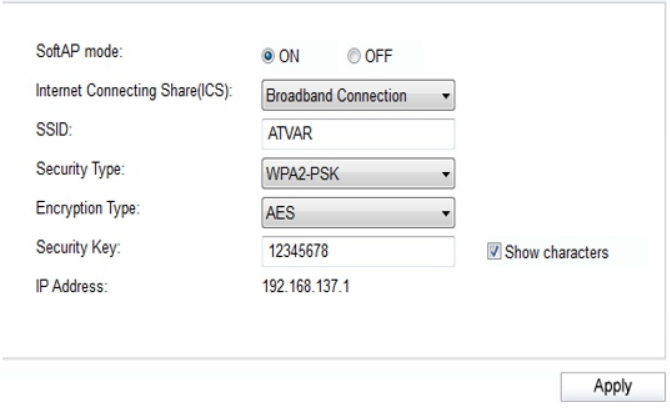


**Fig 9 Broadband command select**

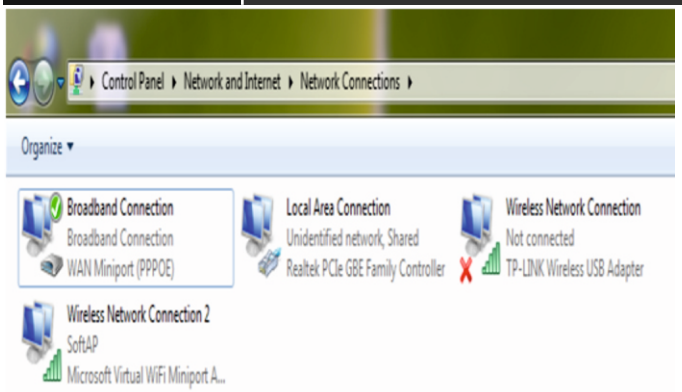


**Fig 10 VPN broadband connection sharing**

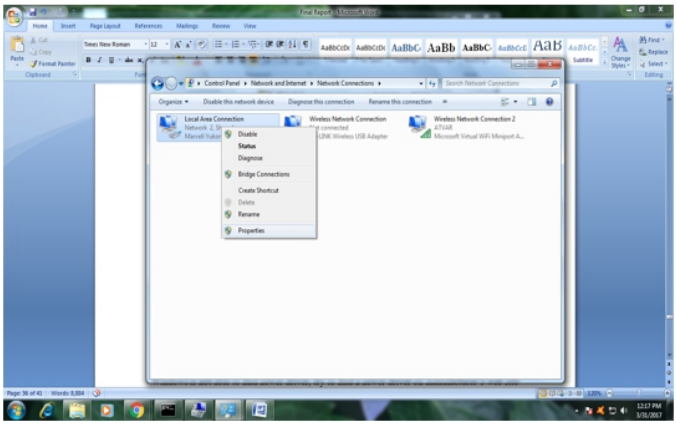

**Fig 11 Open LAN menu select properties**

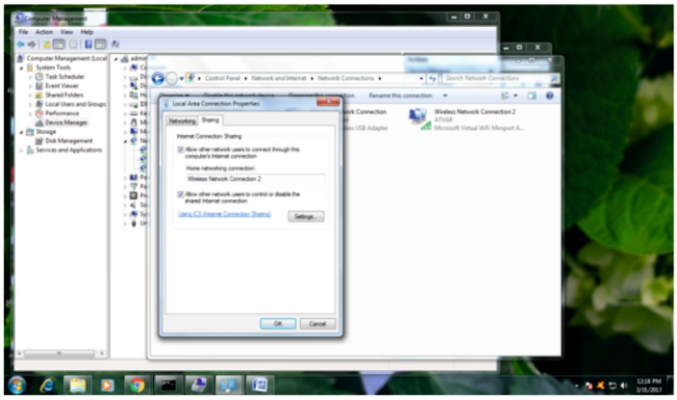

**Fig 12 LAN sharing allow both commands**

I have used "atvar" as new hotspot SSID, and password "12345678". You should change these.

If everything went OK, the last line will show "The hosted network started". In case you receive this:

## III. RESULT

The following method can be used to share your Windows computer's Broadband VPN connection with android mobile.

1. This setup is configured using: Wi-fi router> Computer > Wireless shared network using ATVAR > Network enabled device. The computer using Internet connection sharing will need to have a Wi-fi network adapter for broadcasting the shared wireless network connection 2 connections. This method uses a hosted network that operates using the wireless network adapter's drivers.

2. Launch the command prompt with administrator privileges: In the Start menu, search 'cmd', and when you see the command prompt application, right-click it and select 'Run as Administrator'.

3. In this step, we will run commands to create a virtual hosted network from the wireless network adapter (note that the SSID and password key are examples, we recommend to change them).

   Run the following commands in the admin command prompt.

   Type this exactly,

   hitting "enter" at the end each line:

   netsh wlan set hostednetwork mode=allow ssid=ATVAR key=12345678

   netsh wlan start hostednetwork

   If you performed correctly, the command prompt window will indicate that the hosted network was successfully configured.

   If you encounter errors here, You can verify that your Wi-Fi adapter can perform hosted network operations by running the command

   netsh wlan show drivers

   If you see the line "Hosted Network Supported: Yes", your Wi-Fi card will work.

3. After successfully starting the hosted network, we will then need to share the ATVAR connection to the hosted network. You can do this with the ATVAR TAP adapter (for broadband VPN) or with a manual setup PPTP or L2TP/IPSec connection.

4. Now connect your PC with android phone through wi-fi. The wireless network 2 Hosted network (from step 3, as an example the SSID was ATVAR ). The connecting devices will now be connected through the Broadband VPN connection!

## IV. CONCLUSION

We lives in modern world and still many of us don't have Wi-Fi modem in our house. The reason is Wi-Fi modem/router expensive than the normal VPN- LAN and USB modem. But we do have Wi-Fi feature in our mobile phones. Many times our phones app or games requires big data to be download via 4g or Wi-Fi. 4G is still an expensive connection for average income family users and without a Wi-Fi router we can't actually create a Wi-Fi ad-hoc network. We may have internet in our house but we don't have Wi-Fi router. That time we feel upset. Sometimes at mall, school, collage or offices we gets Wi-Fi networks and we use them. That time we recognize importance of Wi-Fi to download things faster without subscribing for an internet or 3g plan for a mobile separately. As shown in fig 5.1 Wi-Fi working without Wi-Fi router


**Fig 13 Wi-Fi working without Wi-Fi router**

Technology changes within a day. You buy something and the next day you get better stuff for cheaper price. Same way there is a small and cheap Wi-Fi adapter for your pc to create Wi-Fi ad hoc without a Wi-Fi router or modem. If you're not able to buy wireless modem than you should go for Wi-Fi adapter and create a Wi-Fi hotspot in your house. There are many mini USB Wi-Fi adapters available on online stores. But you might get cheaper if you buy from local pc market. I had seen a cheapest Wi-Fi adapter on line. You can find the best one for you and set up your home wireless network.

## REFERENCES

[1] Address Allocation for Private Internets, RFC 1918, Y. Rekhter et al., February 1996

[2] E. Rosen & Y. Rekhter (March 1999). "RFC 2547 BGP/MPLS VPNs". Internet Engineering Task Force (IETF).

[3] Cisco Systems, et al. Internet working Technologies Handbook, Third Edition. Cisco Press, 2000.

[4] International Engineering Consortium. Digital Subscriber Line 2001. Intl. Engineering Consortium, 2001, p. 40.

[5] Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7

[6] Lewis, Mark (2006). Comparing, designing, and deploying VPNs (1st print. ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. ISBN 1587051796

[7] Microsoft Technet. "Virtual Private Networking: An Overview".

[8] Lewis, Mark. Comparing, Designing. And Deploying VPNs. Cisco Press, 2006, p. 5

[9] TechNet Lab. "IPv6 traffic over VPN connections".

[10] Glyn M Burton: RFC 3378 EtherIP with FreeBSD, 03 February 2011

[11] "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)

[12] Soft Ether VPN: Using HTTPS Protocol to Establish VPN Tunnels

[13] "OpenConnect". Retrieved 2013-04-08. OpenConnect is a client for Cisco's AnyConnect SSL VPN OpenConnect is not officially supported by, or associated in any way with, Cisco Systems. It just happens to interoperate with their equipment..

[14] Net-security.org news: Multi-protocol SoftEther VPN becomes open source, January 2014